

## **REMARKS**

Applicant acknowledges, with thanks, the Office Action mailed August 4, 2005. This Amendment and Response is responsive to the Office Action mailed August 4, 2005. The three month shortened statutory period expired November 4, 2005, accordingly a petition and fee for a one month extension are being submitted with this amendment and response. By this amendment, claims 6, 10, 18, 21-23, 43, 46, 51 and 54 have been amended and claims 20, 23, 27-42, 485, 48 and 53 have been canceled.

## **THE REJECTIONS UNDER 35 U.S.C § 102**

Claims 6-59 and 83-86 stand been rejected under Section 102(e) as being anticipated by U.S. Patent Application Publication No. 2002/0007454 to Tarpenning et al. (*hereinafter* Tarpenning). For reasons that will now be set forth, claims 6-7, 9-10, 13-22, 21-22, 24-26, 43-44, 46-47, 49-52, 54-55 and 57-58 in their present condition are not anticipated by Tarpenning.

Independent claims 6, 18, 43 and 51 recite that when a session is initiated a session request is from the initiator to the responder to initiate a new session. The responder generates a new session key pair specifically for the new session (first key pair) comprising a responder public key. The responder sends a session confirm to the initiator with the new responder public key created specifically for the new session. The initiator then generates a new session key pair (second key pair) for specifically created for the new session comprising a new initiator public key. The initiator then sends a key request with the new initiator public key to the responder. Thus, when a new session is initiated between an initiator and a responder, two new session key pairs are generated – one by the initiator and one by the responder, and the two new public keys are exchanged.

By contrast, Tarpenning teaches only one new key pair being created for the session. The new key is created by the responder (authentication server). Referring to paragraph 34, the electronic reader sends its registration ticket to the certificate authority. The registration ticket being previously sent to the reader (see paragraph 32). The authentication server is responsive to receipt of the registration ticket to create a new public/private key pair for the User certificate.

The user certificate (which contains the device private key) is sent to the reader which then installs the private key. The reader reports whether it could install the private key to the authentication server (paragraph 37). “The server receives and stores the success/fail status, and the process completes at steps 865 and 870 respectively, with the reader having an installed User Certificate and the authentication server portion of the process being done.” Thus, Tarpenning only creates one new key pair for the session, whereas as recited in claims 6, 18, 43 and 51 two new key pairs are created for the session, one by the initiator and one by the responder. Therefore, Tarpenning does not show every element of independent claims 6, 18, 43 and 51.

Claims 7, 9-10, 13-37 and 83-86 are directly dependent from claim 6 and therefore contain each and every element of claim 6. Therefore, for the reasons already set forth for claim 6, claims 7, 9-10, 13-37 and 83-86 are not anticipated by Tarpenning.

Claims 19, 21-22 and 24-26 are directly dependent from claim 18 and therefore contain each and every element of claim 18. Therefore, for the reasons already set forth for claim 18, claims 19, 21-22 and 24-26 are not anticipated by Tarpenning.

Claims 44, 46-47 and 49-50 are directly dependent from claim 43 and therefore contain each and every element of claim 43. Therefore, for the reasons already set forth for claim 43, claims 44, 46-47 and 49-50 are not anticipated by Tarpenning.

Claims 54-55 and 57-58 are directly dependent from claim 51 and therefore contain each and every element of claim 51. Therefore, for the reasons already set forth for claim 51, claims 54-55 and 57-58 are not anticipated by Tarpenning.

Furthermore, in addition to the reasons just set forth, claim 84 recites the data package is sent encoded with responder public key and the package confirm is encoded with the initiator public key. As stated hereinabove, Tarpenning does not disclose using two new key pairs, nor does it disclose each party (initiator and responder) encoding messages it sends with its own public key as recited in claim 84.

In addition to the reasons set forth above, claim 85 recites that the responder when the session request is received determines whether a queue limit counter has been exceeded. Furthermore, claim 86 recites aborting the method and writing an error log entry responsive to

exceeding the queue limit counter. There is no teaching in Tarpenning about using a queue counter and aborting if a queue counter is exceeded (Tarpenning only shows checking a sequence number for the existing user certificate to guard against a replay attack – See 960, 965 of Figure 4). Moreover, the word “queue” does not appear anywhere in Tarpenning. Therefore, claims 85-86 are not anticipated by Tarpenning.

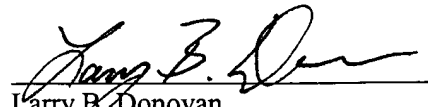
In addition to the reasons set forth above, new claim 87 recites sending a message from the initiator to responder encoded with the new responder public key and sending a message from the responder to the initiator encoded with the new initiator public key. Tarpenning is unable to do this because only the authentication server in Tarpenning creates a new key pair whereas the present invention creates two new keys, one by the initiator (e.g. the device in Tarpenning) and one by the responder (e.g. the authentication server in Tarpenning).

### CONCLUSION

In view of the foregoing it is respectfully submitted that the present claims distinguish over the prior art. If the Examiner believes there are any further matters, which need to be discussed in order to expedite the prosecution of the present application, the Examiner is invited to contact the undersigned.

Respectfully submitted,  
TUCKER ELLIS & WEST LLP

December 5, 2005

  
Larry B. Donovan  
(Registration No. 47,230)  
1150 Huntington Building  
925 Euclid Avenue  
Cleveland, Ohio 44115-1475  
Customer No. 23380  
216-696-3864 (phone)  
216-592-5009 (fax)